Norm eines Ideals und das Symbol $\left(\frac{\alpha}{\mathfrak{P}}\right)_{\mathfrak{m}}$

Sebastian Sura

23. Juli 2017

14.1 Die Norm eines Ideals

Sei $K/\mathbb{Q}$ ein algebraischer Zahlenkörper und sei $D = \mathcal{O}_K$ sein Ganzzahlring. Wir werden in diesem Abschnitt wieder nur nicht-triviale Ideale betrachten.

Definition. Sei $A \trianglelefteq D$ ein Ideal. Wir nennen

$$N_A := N(A) := |D/A| \in \mathbb{N}$$

die *Norm des Ideals* A.

Satz 14.1.1. Sind $A, B \trianglelefteq D$ zwei Ideale, so gilt $N(AB) = N(A)N(B)$.

Beweis. Sind A, B koprim, d.h. $D = A + B$, so gilt $AB = A \cap B$; insbesondere folgt aus 12.3.1

$$D/(AB) \cong D/A \oplus D/B$$

und somit $N(AB) = N(A)N(B)$. Ist $A = P_1^{e_1} \dots P_r^{e_r}$ die Primidealzerlegung von A (vgl. 12.2.8), so gilt also

$$N(A) = \prod_{i=1}^{r} N(P_i^{e_i}),$$

da die Ideale $P_1^{e_1}, \dots, P_r^{e_r}$ paarweise koprim sind. Nach Proposition 12.3.2 gilt weiter

$$N(P_i^{e_i}) = N(P_i)^{e_i},\ i \in \{1, \dots, r\}.$$

Wir erhalten also

$$N\left(\prod_{i=1}^{r} P_i^{e_i}\right) = \prod_{i=1}^{r} N(P_i)^{e_i},$$

insbesondere also $N(AB) = N(A)N(B)$. □

Satz 14.1.2. Angenommen $K/\mathbb{Q}$ sei eine Galois-Erweiterung mit Galoisgruppe $G = \mathrm{Gal}(K/\mathbb{Q})$. Dann gilt für jedes Ideal $A \trianglelefteq D$ schon

$$\prod_{\sigma \in G} A^\sigma = \langle N(A) \rangle .$$

Beweis. Da beide Seiten multiplikativ in A sind, reicht es den Fall zu betrachten, dass $P = A$ ein Primideal ist. Seien $P_1, \dots, P_g$ die paarweise verschiedenen Primideale in $\{P^\sigma \mid \sigma \in G\}$. Das *„Orbit-Stabilizer-Theorem“* liefert dann

$$|G| = g\,|G(P)|,$$

wobei $G(P) = \{\sigma \in G \mid P^\sigma = P\} \leq G$ der Stabilisator von P in G ist. Aus $P \cap \mathbb{Z} \neq 0$, folgt

$$0 \neq P_1 \cap \mathbb{Z} = \dots = P_g \cap \mathbb{Z} = p\mathbb{Z}$$

für eine Primzahl $p \in \mathbb{N}$. In Kapitel 12 §3 haben wir gesehen, dass $e, f \in \mathbb{N}$ existieren dergestalt, dass

$$pD = P_1^e \cdots P_g^e, \quad N(P) = |D/P_1| = \dots = |D/P_g| = p^f$$

und

$$n = [K : \mathbb{Q}] = |G| = efg.$$

Somit gilt $|G(P)| = ef$ und mit Hilfe von Kapitel 12, Theorem 3' und Proposition 12.3.3 erhalten wir

$$\prod_{\sigma \in G} P^{\sigma} = (P_1 \dots P_n)^{ef} = (pD)^f = (p^f)D.$$

□

Satz 14.1.3. Sei $K/\mathbb{Q}$ eine Galois-Erweiterung mit Galois-Gruppe $G = \mathrm{Gal}(K/\mathbb{Q})$. Sei $\alpha \in D$ beliebig und sei $A = \alpha D$ das von α erzeugte Hauptideal. Dann gilt

$$N(A) = |N(\alpha)|.$$

Beweis. Wie gerade gesehen gilt

$$N(A)D = \prod_{\sigma \in G} A^{\sigma} = \prod_{\sigma \in G} (\alpha D)^{\sigma} = \prod_{\sigma \in G} (\alpha^{\sigma})D = \left(\prod_{\sigma \in G} \alpha^{\sigma} \right) D.$$

In Kapitel 12 §1 haben wir bemerkt, dass $\prod_{\sigma \in G} \alpha^{\sigma} = N(\alpha)$, d.h. es gilt

$$N(A)D = N(\alpha)D.$$

Wir haben also zwei ganze Zahlen $N(A), N(\alpha) \in \mathbb{Z}$ die sich nur durch eine Einheit (aus D) unterscheiden, also

$$|N(A)| = |N(\alpha)|.$$

Da $N(A)$ definitionsgemäß stets positiv ist, gilt also $N(A) = |N(A)| = |N(\alpha)|$.
□

Bemerkung 14.1.4. Die Tatsache, dass $N(A) = |N(\alpha)|$ gilt auch ohne die Vorraussetzung, dass $K/\mathbb{Q}$ Galois ist. Der Beweis ist aber um einiges schwerer.

14.2 Das Symbol $\left(\frac{\alpha}{\mathfrak{P}}\right)_m$

Für $m \in \mathbb{N}$ sei D_m der Ganzheitsring von $\mathbb{Q}(\zeta_m)$. Sei $\mathfrak{P} \trianglelefteq_{\mathrm{prim}} D_m$ ein Primideal, welches m nicht enthält und sei $q = N(\mathfrak{P}) = |D_m/\mathfrak{P}|$ seine Norm. Aus Proposition 14.2.3 folgt, dass die Nebenklassen $1 + \mathfrak{P}, \zeta_m + \mathfrak{P}, \dots, \zeta_m^{m-1} + \mathfrak{P}$ paarweise verschieden sind und dass $q \equiv_m 1$ gilt, d.h. $q - 1 \in mD$.

Satz 14.2.1. Sei $\alpha \in D_m \setminus \mathfrak{P}$ beliebig. Dann existiert genau eine Nebenklasse $i + m\mathbb{Z} \in \mathbb{Z}/m\mathbb{Z}$, so dass

$$\alpha^{(q-1)/m} \equiv_{\mathfrak{P}} \zeta_m^i.$$

Beweis. Die multiplikative Gruppe von $F = D_m/\mathfrak{P} \cong \mathbb{F}_q$ ist zyklisch von Ordnung $q - 1$. Nach dem Satz von Lagrange gilt somit für alle $\alpha \in D_m \setminus \mathfrak{P}$ schon

$$\alpha^{q-1} \equiv_{\mathfrak{P}} 1.$$

$\alpha^{(q-1)/m} + P \in F$ ist also eine Nullstelle von

$$X^m - 1 = \prod_{i=0}^{m-1} (X - \zeta_m^i) \in D_m[X]$$

über F, d.h. $\alpha^{(q-1)/m} - \zeta_m^i \equiv_P 0$ für ein $0 \leq i < m$. Da die Nebenklassen der ζ_m^j, $0 \leq j < m$, verschieden sind, ist $i + m\mathbb{Z}$ eindeutig. □

Definition. Sei $\alpha \in D_m$ eine beliebige, algebraische Ganzzahl. Sei weiter $P \trianglelefteq_{\text{prim}} D_m$ ein beliebiges Primideal, welches nicht m enthält. Dann schreiben wir:

$$\left(\frac{\alpha}{P}\right)_m = \begin{cases} 0 & \alpha \in P \\ \zeta & \alpha \notin P \end{cases},$$

wobei $\zeta \in D_m$ die eindeutige m-te Einheitswurzel mit

$$\alpha^{(q-1)/m} \equiv_P \zeta$$

ist.

Satz 14.2.2. Seien $\alpha, \beta \in D_m$ und sei P ein Primideal, welches nicht m enthält. Sei weiter $q = N(P)$.

(a) Es gilt $\alpha^{(q-1)/m} \equiv_P \left(\frac{\alpha}{P}\right)_m$.

(b) Es gilt $\left(\frac{\alpha\beta}{P}\right)_m = \left(\frac{\alpha}{P}\right)_m \left(\frac{\beta}{P}\right)_m$.

(c) Ist $\alpha \equiv_P \beta$, so gilt $\left(\frac{\alpha}{P}\right)_m = \left(\frac{\beta}{P}\right)_m$.

(d) $x^m \equiv_P \alpha$ ist genau dann lösbar, wenn $\left(\frac{\alpha}{P}\right)_m = 1$.

Beweis. (a), (b) und (c) sind klar. Zu (d):
Ist $\alpha \in P$, so sind beide Aussagen stets falsch. Sei also $\alpha \notin P$. Ist $\beta \in D_m$ mit $\beta^m \equiv_P \alpha$, so folgt aus (b) und (c) bereits

$$\left(\frac{\alpha}{P}\right)_m \overset{(c)}{=} \left(\frac{\beta^m}{P}\right)_m \overset{(b)}{=} \left(\frac{\beta}{P}\right)_m^m = 1,$$

da $\left(\frac{\beta}{P}\right)_m$ eine m-te Einheitswurzel ist. Sei nun also umgekehrt $\left(\frac{\alpha}{P}\right)_m = 1$. Dann gilt schonmal $\alpha + P \neq 0 + P \in D_m/P \cong \mathbb{F}_q$, also

$$\alpha \equiv_P \gamma^k,$$

für ein $k \in \mathbb{N}$, wobei $\gamma \in D_m$ modulo P ein zyklischer Erzeuger von $\Gamma = (D_m/P)^*$ ist. Es reicht nun zu zeigen, dass k von m geteilt wird. Aus (a) folgt

$$\alpha^{(q-1)/m} \equiv_P \left(\frac{\alpha}{P}\right)_m = 1,$$

also $\gamma^{k(q-1)/m} \equiv_P 1$. Da γ in Γ die Ordnung $q-1$ hat, folgt daraus

$$q - 1 \mid k(q-1)/m,$$

und somit $k/m \in \mathbb{Z}$, was $m \mid k$ zur Folge hat. □

Korollar. Ist $m \notin P$ ein Primideal und $q = N(P)$, so gilt

$$\left(\frac{\zeta_m}{P}\right)_m = \zeta_m^{(q-1)/m}.$$

Beweis. Aus 14.2.2 (a) folgt diese Gleichung modulo P. Da die Nebenklassen verschiedener m-ter Einheitswurzeln verschieden sind, gilt hier sogar Gleichheit. □

Definition. Sei $A \trianglelefteq D_m$ ein Ideal, welches zu m koprim ist, d.h. $D_m = A + mD_m$. Sei $A = P_1 \cdots P_n$ die Primidealzerlegung von A. Für $\alpha \in D_m$ definieren wir dann

$$\left(\frac{\alpha}{A}\right)_m = \prod_{i=1}^{n} \left(\frac{\alpha}{P_i}\right)_m.$$

Ist $\beta \in D_m$ teilerfrem zu m, so definieren wir

$$\left(\frac{\alpha}{\beta}\right)_m = \left(\frac{\alpha}{\beta D_m}\right)_m.$$

Bemerkung. Da A zu m koprim ist, gilt auch $m \notin P_i$ für alle $1 \leq i \leq m$. Somit ist dies wohldefiniert.

Satz 14.2.3. Seien $A, B \trianglelefteq D_m$ zwei Ideale, die koprim zu m sind und $\alpha, \beta \in D_m$. Dann gelten:

(a) $\left(\frac{\alpha\beta}{A}\right)_m = \left(\frac{\alpha}{A}\right)_m \left(\frac{\beta}{A}\right)_m$,

(b) $\left(\frac{\alpha}{AB}\right)_m = \left(\frac{\alpha}{A}\right)_m \left(\frac{\alpha}{B}\right)_m$ und

(c) Ist A koprim zu α und $X^m \equiv_A \alpha$ lösbar in D_m, so gilt $\left(\frac{\alpha}{A}\right)_m = 1$. Die Umkehrung gilt im Allgemeinen nicht.

Beweis. (a) Die Gleichung ist multiplikativ in A. Wir müssen also nur noch den Fall betrachten, dass A prim ist. Dies wurde gerade in Proposition 14.2.2 (b) gezeigt.

(b) Dies folgt sofort aus der Definition.

(c) Sei $A = P_1 \dots P_n$ die Primidealzerlegung von A. Wegen $A \subseteq P_i$ und $\alpha \notin P_i$ für alle $1 \leq i \leq n$, ist also auch $X^m \equiv_P \alpha$ in D_m lösbar, d.h. $\left(\frac{\alpha}{P_i}\right)_m = 1$ für alle $0 \leq i \leq n$. Somit gilt

$$\left(\frac{\alpha}{A}\right)_m = \prod_{i=1}^{n} \left(\frac{\alpha}{P_i}\right)_m = 1.$$

□

Wir wollen nun untersuchen wie sich $\left(\frac{\alpha}{A}\right)_m$ unter der kanonischen Operation der Galois-Gruppe $G = \mathrm{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q})$ verhält.

Satz 14.2.4. Sei $A \trianglelefteq D_m$ ein Ideal, welches koprim zu m ist und sei $\sigma \in G$. Dann gilt

$$\left(\frac{\alpha}{A}\right)_m^{\sigma} = \left(\frac{\alpha^\sigma}{A^\sigma}\right)_m.$$

Beweis. Da beide Seiten dieser Gleichung multiplikativ in A sind, dürfen wir ohne Einschränkung annehmen, dass $P = A$ ein Primideal ist. Sei $q = N(P)$. Per Definition gilt

$$\alpha^{(q-1)/m} \equiv_P \left(\frac{\alpha}{P}\right)_m .$$

Somit gilt also

$$\left(\frac{\alpha^\sigma}{P^\sigma}\right)_m \equiv_{P^\sigma} (\alpha^\sigma)^{(q-1)/m} \equiv_{P^\sigma} \left(\frac{\alpha}{P}\right)_m^\sigma .$$

Wegen $q = N(P) = N(P^\sigma)$ folgt aus der Eindeutigkeit schon

$$\left(\frac{\alpha}{P}\right)_m^\sigma = \left(\frac{\alpha^\sigma}{P^\sigma}\right)_m ,$$

da $\left(\frac{\alpha}{P}\right)_m^\sigma, \left(\frac{\alpha^\sigma}{P^\sigma}\right)_m$ beide m-te Einheitswurzeln sind. □

Wir wollen abschließend noch das Eisensteinsche Reziprozitätsgesetz benennen. Dazu benötigen wir zuerst einmal einige wichtige Definitionen. Sei dazu $l \in \mathbb{Z}$ eine ungerade Primzahl. In Prop. 13.2.7 wird gezeigt, dass

$$lD_l = (1 - \zeta_l)^{l-1} D_l$$

und dass $(1 - \zeta_l)D_l$ ein Primideal des Grades 1 ist.

Definition. Ein $0 \neq \alpha \in D_m$ wird *primär* genannt, falls es keine Einheit ist, teilerfremd zu l ist und kongruent zu einer ganzen Zahl modulo $(1 - \zeta_l)^2$ ist.

Lemma. Sei $\alpha \in D_l$ eine zu l teilerfremde Ganzzahl. Dann existiert ein $c \in \mathbb{Z}$, welches eindeutig modulo l ist, so dass $\zeta_l^c \alpha$ primär ist.

Beweis. Sei $\lambda = 1 - \zeta_l$. Wir sahen bereits, dass das Primideal λD_l den Grad 1 hat, d.h. es gilt

$$D_l/\lambda D_l \cong \mathbb{F}_l.$$

Insbesondere existieren also für alle $\omega \in D_l$ schon ein $w \in \mathbb{Z}$ mit $\omega \equiv_\lambda w$. Somit existiert also ein $a \in \mathbb{Z}$ mit

$$\alpha \equiv_\lambda a.$$

Da also $(\alpha - a)/\lambda \in D_l$ ganz ist, existiert ein $b \in \mathbb{Z}$, sodass

$$(\alpha - a)/\lambda \equiv_\lambda b.$$

Insbesondere gilt also $\alpha \equiv_{\lambda^2} a + b\lambda$. Aus $\zeta_l = 1 - \lambda$ folgt weiter

$$\zeta_l^c \equiv_{\lambda^2} 1 - c\lambda.$$

Somit gilt

$$\zeta_l^c \alpha \equiv_{\lambda^2} a + (b - ac)\lambda.$$

Da $\lambda^{l-1} \sim l$ gilt, gilt also auch $a \equiv_\lambda \alpha \not\equiv_\lambda 0$ und a ist wie α koprim zu l. Sei daher $c \in \mathbb{Z}$ die Lösung der Gleichung $ax \equiv_l b$. Dann ist

$$\zeta_l^c \alpha \equiv_{\lambda^2} a$$

und $\zeta_l^c \alpha$ ist primär. Sei nun $\tilde{c} \in \mathbb{Z}$ eine weitere solche Lösung, d.h.

$$b - a\tilde{c} \equiv_\lambda 0 \equiv_\lambda b - ac.$$

Da a teilerfremd zu λ ist, gilt $c \equiv_\lambda \tilde{c}$, d.h. $\lambda \mid c - \tilde{c}$. Somit gilt $c - \tilde{c} \in \lambda D \cap \mathbb{Z} = l\mathbb{Z}$, d.h. $c \equiv_l \tilde{c}$. □

Theorem 1 (Das Repiprozitätsgesetz von Eisenstein)**.** Seien $l \in \mathbb{Z}$ eine ungerade Primzahl, $a \in \mathbb{Z}$ teilerfremd zu l und $\alpha \in D_l$ primär. Angenommen α und a seien koprim, dann gilt

$$\left(\frac{\alpha}{a}\right)_l = \left(\frac{a}{\alpha}\right)_l$$

Beweis. Dies wird im fünften Abschnitt mit Hilfe der *Stickelberger Relationen* bewiesen. □